Idaho National Engineering and Environmental Laboratory

Technology Highlight:

Digital Signatures for Data Base Structures

Problem Description:

For modern industry to migrate to true paperless operations, a trusted means for creating "electronic signatures" must be available. The electronic signature mechanism must include non-repudiation (validation of both signatures and the original data signed). Currently, electronic signature for "flat files" (such as e-mail messages) can be implemented using off the shelf technology, governed by industry standards. This is achievable because a flat file, as a single entity, contains all of the data being signed and verified. The electronic signature becomes an inseparable part of that file, much in the same way that a written signature becomes a part of a document. Use of electronic signature technology is growing significantly as more information is exchanged on Internet/Intranets. Most currently acceptable electronic signature systems incorporate the Public/Private Key Infrastructure (PKI). These PKI based electronic signatures are becoming legally valid "signatures" for several government agencies (FDA, State Government, DOE/DOD pending, etc).

The need to "sign" information, and provide non-repudiation, is not limited to the information contained in flat files. Much of the data that is subject to review and approval resides in relational databases instead of flat-files. A database electronic signature is not extended to the entire database (access control) or just an individual table record (flat) – but to records crossing complex entities within that database (an individual form being approved). There is no known industry-wide solution to sign database entities (forms) and still provide non-repudiation of the signature relative to the original data stored in a relational structure. (Examples: Government or corporate data with legal significance, engineering design archives with PE signatures, procurement and work approval databases, IRS tax returns.) The technology of printing computer reports, signing the paper, and filing or scanning the documents only increases paper production. A digital signature technology must be provided to move many common business processes to a truly efficient, paperless state.

Solution Description:

INEEL is developing technology to extend industry standard algorithms to database structures. This technology provides electronic signature for database records, ensuring data integrity, user authenticity, and non-repudiation for signatures related to specific data base values. Currently the technology is implemented in an INEEL inventory-processing system that is used to collect and certify information about the hazardous waste located at the INEEL. DOE and the state of New Mexico have accepted this implementation of electronic signature for use in the characterization, certification, and transfer of this waste from the INEEL to the Waste Isolation Pilot Plant.

As the INEEL implements additional functionality to the inventory processing system, the electronic signature capability will be expanded.

Opportunity

The INEEL developed digital signatures for data base structures because no commercial solutions were available. With further development, this technology can be applied to solve similar problems for government customers or migrated into a commercially viable product. The solution is independent of vendor database and easily transferable between different database applications that require non-repudiation.

Business contact:
Toni Austin
208-526-3140
ama@inel.gov

Technical contacts:
Ben Groeneveld
208-526-4352
bjg@inel.gov

Wayne Austad
208-526-5423
wqa@inel.gov

Stuart Walsh
208-526-5125
walssc@inel.gov